Kit Bit4id

Instalación y manual de Usuario para Mac OS X

Bit4id Ibérica
C/ Marie Curie, 8-14
Forum Nord de Tecnología
08042 – Barcelona
España
Tel. +34 935 35 35 18
info.es@bit4id.com

Bit4id Italia
Via Coroglio, 57
Città della Scienza
80124 Napoli
Italia
Tel. +39 081 762 56 00
info.it@bit4id.com

Bit4id UK
2 London Wall Buildings
London Wall,
London EC2M 5UU
United Kingdom
Tel. +44 (0) 203 397 3166
info.uk@bit4id.com

Bit4id Perú
Avda. Olavegoya, nº 1835
Distrito Jesus Maria
Lima 11
Perú
Tel: +51 947 744 704
info.pe@bit4id.com

Oficina Lisboa
Rua Cesário Verde, 32
2790-495 Queijas (Lisboa)
Portugal
Tel .+351 914 58 30 21
info.pt@bit4id.com

Oficina Milán
Corso Vercelli, 11
20144 Milano
Italia
Tel. +39 024 547 42 59
info.it@bit4id.com

Oficina Guatemala
15 avenida, 14-09 zona 10
Oakland - 01010
Guatemala
Guatemala
Tel: +502 22 21 91 63
aor@bit4id.com

qualityaustria
SYSTEM CERTIFIED
ISO 9001:2008 No.07974/0
ISO 14001:2004 No.01608/0

ISO 9001:2008
ISO 14001:2004
ISO 27001:2005

Sumario

Revisiones 3
Introducción 4
A quién va dirigido este documento 4
Antes de comenzar 4
Instalación 5
Instalación manual de Bit4id Middleware 7
Problemas conocidos 8
Configuración en Firefox 8
Antes de comenzar a usar el Kit Bit4id 10
Uso de PIN Manager 10
Funcionalidades 10
Tabla de funciones 10
Preguntas frecuentes 12
Glosario 13

Revisiones

Revisión	Fecha	Cambios	Autor
1.0	06/11/2012	Primera redacción	RLG
1.1	09/11/2012	FAQ	GSA
1.2	12/11/2012	Revisión y aprobación	RLG
1.3	14/11/2012	Revisión estructura	RLG
1.4	19/11/2012	Adaptación para todo tipo de lectores	GSA

Introducción

Este manual sirve de guía para llevar a cabo de manera exitosa el proceso de instalación del Kit Bit4id, para el uso de tarjetas criptográficas, y el procedimiento para acceder y usar la aplicación de gestión. El Kit Bit4id consta de los siguientes componentes:

- **Bit4id Middleware**: librerías que permiten a cualquier aplicación del Sistema Operativo operar con las tarjetas criptográficas mencionadas
- **Bit4id PIN Manager**: aplicación para la gestión de la tarjeta, que permite realizar operaciones como cambio de PIN o PUK, desbloqueo de PIN, obtener información sobre la tarjeta,...

Este manual le guiará de una manera sencilla en el proceso de instalación y uso del Kit Bit4id.

A quién va dirigido este documento

- ***Usuarios finales***, que van a utilizar tarjetas con chip en entornos Mac OS X.

Antes de comenzar

Asegúrese de disponer de:

- Un lector de tarjetas estándar, compatible PC/SC que se encuentre correctamente conectado, instalado y configurado. Siga las instrucciones suministradas por el fabricante del lector para verificar su correcta instalación y funcionamiento.
- Disponer de la última versión del Kit Bit4id.
- Para poder realizar la instalación, es indispensable poseer permisos de Administrador. En caso de no poseerlos la instalación será denegada.

Instalación

Descargue el instalador desde la página adecuada del Proveedor de Servicios de Certificación que le ha suministrado la tarjeta criptográfica y ejecútelo en su equipo. Si se le solicita, permita la ejecución de la aplicación.

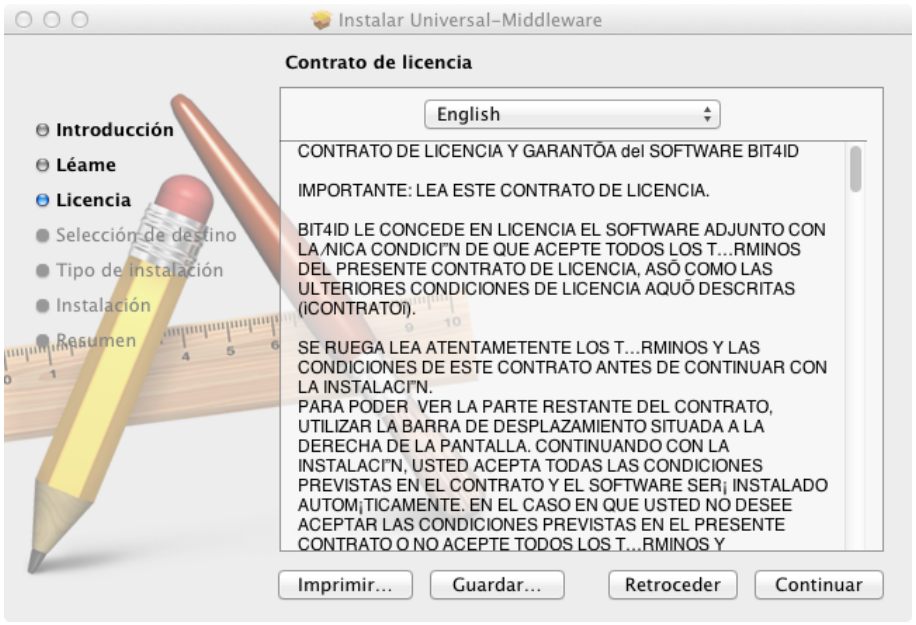
Hacer doble click sobre el icono del instalador, *Universal-Middleware.pkg*.

Se lanzará el instalador. Hacer click en *Continuar*.

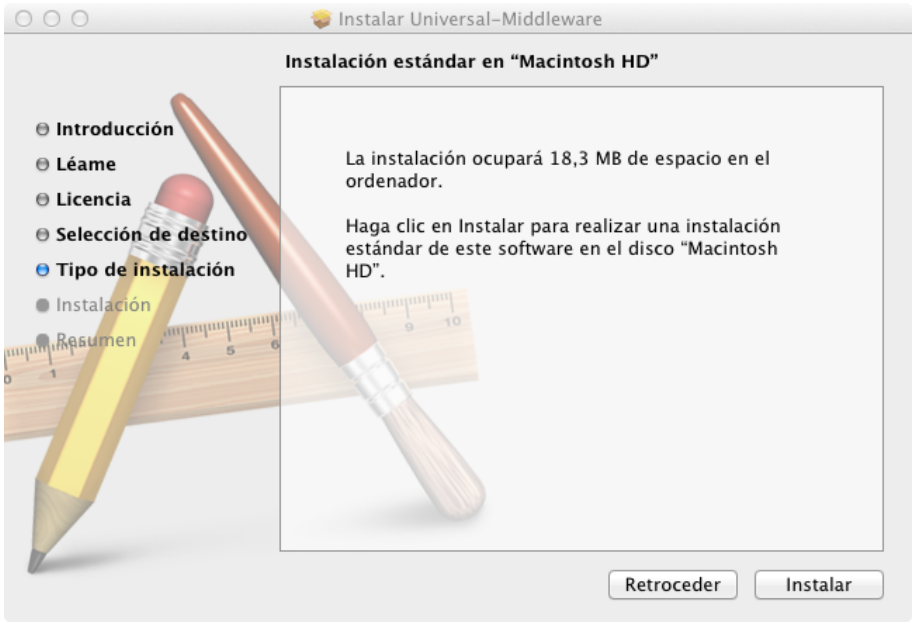
En el siguiente paso, revisar las instrucciones de instalación y hacer click en *Continuar*.

Instalar Universal-Middleware
Información importante
Introducción
Léame
Licencia
Selección de destino
Tipo de instalación
Instalación
Resumen
"Universal Middleware para Mac OS X"
"Universal Middleware for Mac OS X"
Castellano
Una vez completada la instalación, es necesario reiniciar el sistema.
Este software requiere un lector de tarjetas inteligentes compatible con el componente Apple Smartcard Services correctamente instalado y configurado en el sistema.
Este paquete instala el soporte para el navegador Safari. También instala la librería PKCS#11, para usar con programas como Mozilla Firefox.
La librería PKCS#11 se instalará en la siguiente ruta:
/System/Library/Bit4id/pkcs11/libbit4ipki.dylib
Para la instalación de la librería PKCS#11 en Mozilla Firefox o en otras aplicaciones, es necesario utilizar esta
Imprimir...
Guardar...
Retroceder
Continuar

A continuación se presenta el acuerdo de licencia.

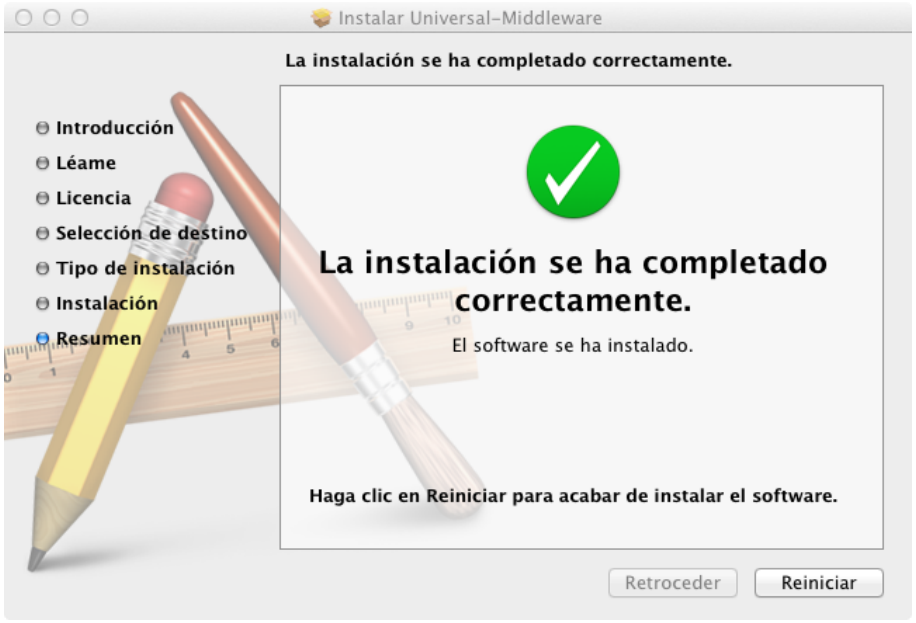

Instalar Universal-Middleware
Contrato de licencia
Introducción
Léame
Licencia
Selección de destino
Tipo de instalación
Instalación
Resumen
English
CONTRATO DE LICENCIA Y GARANTÕA del SOFTWARE BIT4ID
IMPORTANTE: LEA ESTE CONTRATO DE LICENCIA.
BIT4ID LE CONCEDE EN LICENCIA EL SOFTWARE ADJUNTO CON LA ⁄NICA CONDICI"N DE QUE ACEPTE TODOS LOS T...RMINOS DEL PRESENTE CONTRATO DE LICENCIA, ASÕ COMO LAS ULTERIORES CONDICIONES DE LICENCIA AQUÕ DESCRITAS (¡CONTRATO¡).
SE RUEGA LEA ATENTAMETENTE LOS T...RMINOS Y LAS CONDICIONES DE ESTE CONTRATO ANTES DE CONTINUAR CON LA INSTALACI"N.
PARA PODER VER LA PARTE RESTANTE DEL CONTRATO, UTILIZAR LA BARRA DE DESPLAZAMIENTO SITUADA A LA DERECHA DE LA PANTALLA. CONTINUANDO CON LA INSTALACI"N, USTED ACEPTA TODAS LAS CONDICIONES PREVISTAS EN EL CONTRATO Y EL SOFTWARE SER¡ INSTALADO AUTOM¡TICAMENTE. EN EL CASO EN QUE USTED NO DESEE ACEPTAR LAS CONDICIONES PREVISTAS EN EL PRESENTE CONTRATO O NO ACEPTE TODOS LOS T...RMINOS Y
Imprimir...
Guardar...
Retroceder
Continuar

Es importante permitir que se realice la instalación estándar, en el directorio predeterminado, para simplificar la configuración. Hacer click en *Instalar*.



Se solicitará acceso de administrador al equipo, dado que se van a instalar y configurar librerías de importancia.

La instalación ha concluido con éxito:



Instalación manual de Bit4id Middleware

En este punto se describe los pasos necesarios para la instalación manual, mediante la copia de las librerías en los directorios requeridos. El interfaz PKCS#11 de Bit4id Middleware para Mac OS X está constituido por dos archivos:

`libbit4ipki.dylib.conf`

`libbit4ipki.dylib`

Los dos archivos se copian siempre juntos en la misma carpeta de librerías que dependerá de la versión utilizada. Por ejemplo:

`/System/Library/Bit4id/pkcs11`

Problemas conocidos

La librería puede ser utilizada con Mozilla Firefox para una autenticación client SSL.

No obstante, un bug de Mozilla impide especificar la ruta de la librería utilizando la interfaz gráfica; de hecho podría suceder que después de haber seleccionado la librería, Firefox visualice una ruta del tipo:

AAAAAAFWAAIAAAxNYWNpbnRvc2ggSEQAAAAAAAAAAAAAAAAAAAC

Para evitar el problema, es necesario introducir manualmente la ruta completa de la librería en el campo en cuestión, por ejemplo:

```
/System/Library/Bit4id/pkcs11/libbit4ipki.dylib
```

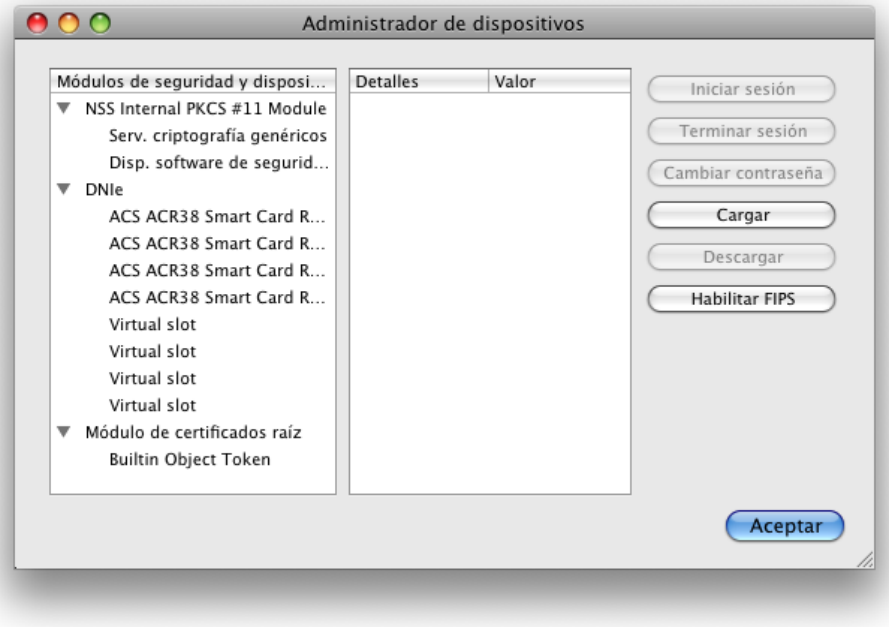
Configuración en Firefox

Para poder utilizar la tarjeta inteligente en el navegador Mozilla Firefox es necesario incorporar el soporte a las librerías del Universal Middleware de forma manual. Este procedimiento solo debe realizar si la instalación automatizada ha fallado.

Tras abrir Mozilla Firefox, se debe hacer click en *Firefox* → *Preferencias*

A continuación, seleccionar la pestaña *Cifrado* y hacer click en *Dispositivos de Seguridad*

En la pantalla del Administrador de dispositivos de seguridad, hacer click en el botón Cargar.



En la ventana *Cargar dispositivo PKCS#11* se deben introducir los siguientes datos:

- Nombre del módulo: *Bit4id Universal Middleware*
- Archivo del módulo: `/System/Library/Bit4id/pkcs11/libbit4ipki.dylib`

A continuación, hacer click en *Aceptar*. El módulo se incorporará satisfactoriamente, y la instalación en Firefox habrá concluido.

Antes de comenzar a usar el Kit Bit4id

Bit4id PIN Manager requiere un lector de tarjetas inteligentes estándar, compatible PC/SC, que se encuentre correctamente conectado, instalado y configurado antes de comenzar.

Siga las instrucciones suministradas por el fabricante del lector para verificar su correcta instalación y funcionamiento.

Uso de PIN Manager

La aplicación Bit4id PIN Manager está disponible dentro del menú Aplicaciones.

Funcionalidades

Bit4id PIN Manager dispone de múltiples funcionalidades, accesibles desde la pantalla principal:

[Imagen 1]

Tabla de funciones

La siguiente tabla resume las funciones expuestas en la pantalla principal de Bit4id PIN Manager.

Función	Descripción
Cambiar PIN	Función para cambiar el PIN de la tarjeta (ver imagen 2)
Desbloquear PIN	Función para desbloquear el PIN de la tarjeta mediante el PUK de la misma (ver imagen 3)
Cambiar PUK	Función para cambiar el PUK de la tarjeta (ver imagen 4)
Información de la tarjeta	Ventana que muestra información sobre la tarjeta (modelo, número de serie, identificación del fabricante y etiqueta) (ver imagen 5)

Cambiar PIN

Introduzca el PIN antiguo de la tarjeta y el nuevo PIN. El nuevo PIN tiene que tener entre 6 y 8 dígitos alfanuméricos.

[Imagen 2]

Desbloquear PIN

Para desbloquear el PIN, introduzca el PUK de la tarjeta e introducir el nuevo PIN. El nuevo PIN tiene que tener entre 6 y 8 dígitos alfanuméricos.

[Imagen 3]

Cambiar PUK

Introduzca el PUK antiguo de la tarjeta y el nuevo PUK. El nuevo PUK tiene que tener entre 6 y 8 ígitos alfanuméricos.

[Imagen 4]

Información de la tarjeta

Ofrece información detallada de la tarjeta: modelo, número de serie, fabricante y etiqueta.

Preguntas frecuentes

¿Puedo combinar números y letras para el número PIN de la tarjeta?

Sí, no hay ningún problema, siempre que el nuevo PIN tenga entre 6 y 8 dígitos.

¿Existe un máximo de inserciones de PIN en el caso de que tenga alguna duda y no recuerde mi número PIN? ¿Cuándo puede quedar bloqueada la tarjeta?

Si inserta más de 3 veces el código PIN de forma errónea, este se bloquea. Póngase en contacto con Bit4id para desbloquearlo.

¿Existe un máximo de inserciones de PUK para intentar desbloquear el PIN? ¿Qué ocurre si la tarjeta queda bloqueada?

Si inserta más de 3 veces el código PUK de forma errónea, este se bloquea. Por razones de seguridad, la tarjeta se bloquea completamente. Póngase en contacto con Bit4id.

Glosario

Autoridad de Certificación: Es la entidad de confianza, responsable de emitir y revocar los certificados electrónicos, utilizados en la firma electrónica. La Autoridad de Certificación, por sí misma o mediante la intervención de una Autoridad de Registro, verifica la identidad del solicitante de un certificado antes de su expedición o, en caso de certificados expedidos con la condición de revocados, elimina la revocación de los certificados al comprobar dicha identidad.

Caducidad del certificado digital: El certificado digital tiene un período de vigencia que consta en el mismo certificado. Generalmente es de 2 años, aunque por ley se permite una vigencia de hasta 5 años. Una vez el certificado haya caducado, no se podrán utilizar los servicios ofrecidos por la Administración que requieran firma electrónica, y cualquier firma electrónica que se haga a partir de ese momento no tendrá validez.

Certificado digital: Documento en soporte informático emitido y firmado por la Autoridad de Certificación, que garantiza la identidad de su propietario.

Certificado reconocido: Certificado expedido por un Prestador de Servicios de Certificación que cumple los requisitos establecidos en la Ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten, de conformidad con lo que dispone el capítulo II del Título II de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

Firma electrónica: Conjunto de datos, en forma electrónica, anejos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge. Existen 3 tipos de firma electrónica: firma electrónica simple, avanzada y reconocida.

Firma electrónica simple: Conjunto de datos, en forma electrónica, anejos a otros datos.

Firma electrónica avanzada: Firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.

Firma electrónica reconocida: Se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma. La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.

Función hash: es una operación que se realiza sobre un conjunto de datos de cualquier tamaño, de forma que el resultado obtenido es otro conjunto de datos de tamaño fijo, independientemente del tamaño original, y que tiene la propiedad de estar asociado unívocamente a los datos iniciales, es decir, es imposible encontrar dos mensajes distintos que generen el mismo resultado al aplicar la Función hash.

Hash o Huella digital: Resultado de tamaño fijo que se obtiene tras aplicar una función hash a un mensaje y que cumple la propiedad de estar asociado unívocamente a los datos iniciales.

Integridad: La integridad es la cualidad que posee un documento o archivo que no ha sido alterado y que además permite comprobar que no se ha producido manipulación alguna en el documento original.

Listas de Revocación de Certificados o Listas de Certificados Revocados: Lista donde figuran exclusivamente las relaciones de certificados revocados o suspendidos (no los caducados).

No repudio: El emisor que firme electrónicamente un documento no podrá negar que envió el mensaje original, ya que éste es imputable al emisor por medio de la clave privada que únicamente conoce él y que está obligado a custodiar. El no repudio permite, además, comprobar quién participó en una transacción.

El no repudio o irrenunciabilidad es un servicio de seguridad estrechamente relacionado con la autenticación y que permite probar la participación de las partes en una comunicación. La diferencia esencial con la autenticación es que la primera se produce entre las partes que establecen la comunicación y el servicio de no repudio se produce frente a un tercero

Prestador de Servicios de Certificación o PSC: Persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica. Ver Autoridad de Certificación.

PIN: Secuencia de caracteres que permiten el acceso a los certificados. Número de Identificación Personal, en ocasiones llamado NIP.

PUK: Secuencia de caracteres que permiten el cambio o desbloqueo del PIN. Clave Personal de Desbloqueo.

Renovación: La renovación consiste en solicitar un nuevo certificado mediante un certificado vigente pero que está a punto de caducar. De esta manera, antes de la caducidad de un certificado se puede solicitar la renovación y esto implica que se emita un nuevo certificado válido.

Revocación: Anulación definitiva de un certificado digital a petición del suscriptor, o por propia iniciativa de la Autoridad de Certificación en caso de duda de la seguridad de las claves. La

revocación es un estado irreversible. Se puede solicitar la revocación de un certificado después de una situación de suspensión o por voluntad de las personas autorizadas a solicitarla. De la misma manera, en el caso de un certificado suspendido, si ha pasado el periodo de suspensión máximo, si el certificado no ha sido habilitado, pasa a estar definitivamente revocado. Cuando la entidad de certificación revoca o suspende un certificado, ha de hacerlo constar en las Listas de Certificados Revocados (CRL), para hacer público este hecho. Estas listas son públicas y deben estar siempre disponibles.

Tarjeta inteligente (smartcard): Cualquier tarjeta con circuitos integrados que permiten la ejecución de cierta lógica programada.